REMARKS/ARGUMENTS

Claim Status

Claims 1, 3-10, 12 and 13 are now pending, with claims 1 and 12 being in independent form. Dependent claims 2 and 11 have been canceled. Independent claims 1 and 12 have been amended to incorporate the subject matter of canceled dependent claim 2. Additional support for the amendments may be found, for example, at pg. 8, lines 27-31 and pg. 8, line 36 to pg. 9, line 3 of the specification as originally filed. No new matter has been added. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

Claim 11 stands rejected under 35 U.S.C. §101 as directed to non-statutory subject matter. Claim 11 has been canceled. This rejection is therefore moot.

Claims 1-13 stand rejected under 35 U.S.C. §103(a) as unpatentable over "Clustering Intrusion Detection Alarms to Support Root Cause Analysis", IBM Research, Zurich Research Laboratory, ACM Transactions on Information System Security, Vol. 6, No. 4, pgs. 443-474, November 2003 ("*Julisch*") in view of U.S. Pub. No. 2004/0044912 ("*Connary*").

Applicants have carefully considered the Examiner's rejections, and the comments provided in support thereof. For the following reasons, applicants respectfully assert that all claims now pending in the present application are patentable over the cited art.

Patentability of the Independent Claims Under 35 U.S.C. §102(a)

Independent claim 1 has been amended to incorporate the subject matter of dependent claim 2 (now canceled). Amended independent claim 1 now recites, *inter alia*, "consulting the

complete alerts by at least one of successively interrogating and browsing said complete alerts so that the alert management system responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request to enable said request to be refined, said request being a logic formula of at least one of said valued attributes". Independent claim 12 has been correspondingly amended. Support for the amendments may be found, for example, at pg. 5, lines 1-13 of the specification as originally filed. No new matter has been added.

The Examiner (at pgs. 5-6 of the Office Action) acknowledges that *Julisch* does not disclose "each complete alert is saved in the logic file system as a file with a completed description of each complete alert expressed using propositional logic," as recited in independent claims 1 and 12, and cites *Connary* for this feature.

Applicants respectfully disagree that the combination of *Julisch* and *Connary* either teaches or suggests applicants' claimed invention as recited in now amended independent claims 1 and 12.

Connary (paragraph [0008], lines 1-8) describes "[a] system ... [that] comprises a management module and at least one event module. In addition, the system can comprise at least one sensor. The sensor detects network events and records data regarding such events. For example, the event data can comprise the name or Internet protocol (IP) address of the sensor reporting the event, the type of sensor reporting the event, and/or the protocol (e.g., TCP/IP or UDP) used by the sensor". *Connary* (paragraph [0008], lines 16-20) additionally explains that "[t]he event module is coupled to the sensor to receive the event data therefrom. The event module can normalize the event data into a uniform format and can store this data for

- 7 -

transmission to the management module". *Connary* (paragraph [0010], lines 1-2) further explains that "[t]he management module uses the event data to determine threat level data".

Connary thus teaches a system for managing alerts that comprises a management module and at least one event module. A sensor detects network events and records data regarding the events, such as the name or Internet protocol address of the reporting sensor. The event module receives the event data from a sensor and normalizes this data into a uniform format before transmission to the management module. The management module then uses the received event data to determine threat levels associated with at least one event.

Connary, however, fails to teach or suggest that complete alerts (or complete alarms) are saved in a logic file system with a completed description of each complete alert using propositional logic. Indeed, *Connary* has nothing whatsoever to do with complete alerts within the meaning of applicants' claimed invention, i.e., alerts having a description that includes a conjunction of valued attributes belonging to attribute domains. Rather, *Connary* is directed to detected alarms that have a uniform format.

The Examiner asserts that paragraphs [0092] and [0097] of *Connary* disclose applicants' claimed limitation. Applicants disagree with this assertion. *Connary* (paragraph [0091]; FIG. 5) explains that "the event data processor 64 receives and normalizes the event data 38 into a uniform format". Paragraph [0092] of *Connary* provides a description of the normalization step(s) performed by the event module. However normalizing the format of event data has nothing to do with generalizing the attributes of detected alerts.

In addition, *Connary* (paragraph [0097], lines 1-9) explains that "[a] rule engine 78 can apply user-specified rules to determine whether to set or reset a security alarm generated for the user via the GUI 62. For example, the user can indicate that if the threat level(s) of the threat

level data equals or exceeds a user-specified level, then the rule engine 78 generates alert data 42 to trigger an alarm for the user via the GUI 62. Conversely, if the threat level data is less than the user-specified level, then the rule engine 78 generates the alert data 42 so that the alarm is reset or remains inactivated". This section of *Connary* merely describes how threat levels are defined.

Moreover, even assuming, *arguendo*, that *Connary* teaches that *Boolean logic operators or mathematical functions* are utilized for <u>generating</u> the threat level data, as explained at lines 10-20 of paragraph [0097], there is no teaching, suggestion or slightest hint of whether and/or how complete alerts should be <u>saved</u> in a logic file system. As described at pg. 5, lines 1-3 of applicants' disclosure, the claimed logic system may comprise an LISFS, which is disclosed in a paper by Padioleau and Ridoux entitled "A Logic File System" that was presented at the Usenix Annual Technical Conference in 2003. Independent claims 1 and 12 each specify <u>how</u> complete alerts are <u>stored</u>, i.e., each complete alert is saved in the logic file system as a file with a completed description of each complete alert <u>expressed using propositional logic</u>. *Connary* <u>fails</u> to teach or suggest this express and important limitation.

Storing complete alerts in a logic file system in the manner recited in independent claims 1 and 12 advantageously enables a security operator to consult an alert management system in an efficient, quick and flexible manner to obtain a precise view of all alerts issued by intrusion detection sensors (see pg. 2, lines 33-37 of the instant specification). Moreover, the stored complete description is expressed using <u>propositional logic</u>. As a result, it is possible to more efficiently and advantageously consult complete alerts and/or to successively browse the alerts in the set of complete alerts. *Connary* <u>fails</u> to teach or suggest applicants' claimed invention that encompasses such advantageous features and functionality. *Connary* <u>fails</u> to teach or suggest

that each complete alert is saved in a logic file system as a file with a completed description expressed using propositional logic.

Moreover, the subject matter of now-canceled claim 2 has been added to independent claim 1, which now recites, *inter alia*, the additional step of "consulting the complete alerts by at least one of successively interrogating and browsing said complete alerts so that the alert management system responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request to enable said request to be refined, said request being a logic formula of at least one of said valued attributes". Independent claim 12 now recites a corresponding limitation. The Examiner asserts that *Julisch* discloses this feature.

Applicants disagree that the combination of *Julisch* and *Connary* teaches or suggests anything about consulting by browsing and interrogating complete alerts that are stored in a logic file system, or requests for complete alerts that comprise a logic formula of valued attributes.

Julisch (pg. 464) discloses Table II that includes generalized alarms of an alarm cluster. *Julisch* (pg. 465) provides a description of the contents of this table. More particularly, *Julisch* (pg. 464) depicts a table that includes generalized alarms of the alarm cluster. *Julisch* (pg. 465) explains the meaning of several examples of generalised alarms, e.g., WWW ITS *View Source Attack*, FTP SYST *Command Attempt*, which are contained in Table II shown at pg. 464.

Julisch (pg. 465, lines 12-13) provides the expression:

"GET /search_cgi/cgi?action=View&VdkVgwKey=http%3A%2Fwww%2Exyz%2Ecom"

However, this expression has nothing to do with a request for consulting a complete alert in a logic file system. *Julisch* (pg. 465, lines 10-24) merely describes an example of the alarm type *WWW IIS View Source Attack*. Here, a search engine returns URLs having a coding error

"%2E" (instead of a "dot") in response to client requests. Each time that a client clicks on one of the returned search results, a *WWW IIS View Source Attack* alarm is triggered. That alarm can also be triggered by internal clients requesting external web pages, the URL of which has a coding error ("%2E"). Accordingly, the "GET . . . com" expression simply corresponds to a web page link that is generated by a defective search engine. There is nothing at pg. 465 of *Julisch* relating to interrogating or browsing complete alerts in Table II shown at pg. 464 of *Julisch*. The only request that is disclosed is a client <u>web page request,</u> which differs substantially from what applicants' have disclosed and claimed.

Moreover, *Julisch* (section 7, pgs. 467-468) provides a summary of the main steps for performing the disclosed alert management method, i.e., detecting alarms, performing alarm clustering and attribute generalization. Applicants' claimed invention, however, enables a user, in response to valued attributes, to obtain a quick overview of relevant triggered alerts in generalized form. *Julisch* <u>fails</u> to teach or suggest applicants' claimed invention that encompasses such advantageous features and functionality.

Julisch and/or *Connary*, whether considered individually or in combination, thus <u>fail</u> to teach or suggest the express recitations of independent claims 1 and 12.

Reconsideration and withdrawal of the rejection of claims 1 and 12 as unpatentable over the combination of *Julisch* and *Connary* under 35 U.S.C. §103 are accordingly deemed to be in order, and early notice to that effect is solicited.

Dependent Claims

In view of the patentability of independent claims 1 and 12 for the reasons presented above, each of dependent claims 2-10 and 13 is respectfully deemed to be patentable therewith

over the prior art. Moreover, each of these claims includes features which serve to still further distinguish the claimed invention over the applied art.
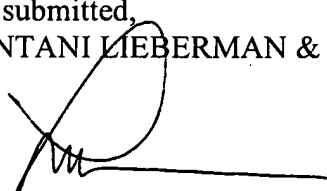
Conclusion

Based on all of the above, applicants submit that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are once more solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned to facilitate an early resolution of any outstanding issues.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By _____
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: April 21, 2009